Daniel Srourian, Esq.
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Counsel for Plaintiff Dreger

Patrick A. Barthle
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 229-4023
pbarthle@forthepeople.com

Ryan D. Maxey
Florida Bar No.: 0059283
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
Telephone: (813) 448-1125
Email: ryan@maxeyfirm.com

Counsel for Plaintiff Boyd

Jason R. Hull [11202]
jhull@mohtrial.com
MARSHALL OLSON & HULL, PC
Newhouse Building
Ten Exchange Place, Suite 350
Salt Lake City, Utah 84111
Telephone: 801.456.7655

Gary M. Klinger*
gklinger@milberg.com
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878

Attorneys for Plaintiff Ralph Maddox

Jared D. Scott (#15066)
ANDERSON & KARRENBERG
50 West Broadway, #600
Salt Lake City, UT 84101-2035
Telephone: (801) 534-1700
jscott@aklawfirm.com

Richard Lyon
rick@dovel.com
DOVEL & LUNER, LLP
201 Santa Monica Blvd., Suite 600
Santa Monica, California 90401
Telephone: (310) 656-7066

Attorneys for Plaintiff Dawn Davis

Jared D. Scott (#15066)
ANDERSON & KARRENBERG
50 West Broadway, #600
Salt Lake City, UT 84101-2035
Telephone: (801) 534-1700
jscott@aklawfirm.com

Kenneth J. Grunfeld (Pro Hac Vice)
KOPELOWITZ OSTROW, P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Telephone: (954) 525-4100
grunfeld@kolawyers.com

Attorneys for Plaintiff Tyler Whitmore

Jason R. Hull [11202]
jhull@mohtrial.com
MARSHALL OLSON & HULL, PC
Newhouse Building
Ten Exchange Place, Suite 350
Salt Lake City, Utah 84111
Telephone: 801.456.7655

Mason A. Barney*

mbarney@sirillp.com
Tyler J. Bean*
tbean@sirillp.com
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: 212.532.1091

Attorneys for Plaintiffs Williams, Robinson, and Ryan

Charles H. Thronson
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, Utah 84111
Telephone: (801) 532-1234

William B. Federman
wbf@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560

Counsel for Plaintiff Marty Alexander

Ashton J. Hyde
YOUNKER HYDE MACFARLANE, PPLC
250 E. 200 South, Suite 1100
Salt Lake City, UT 84111
Telephone: (801) 335-6467
ashton@yhmlaw.com

Terence R. Coates
Dylan J. Gould
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 665-0204
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff Stephen Hawes

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF UTAH

In re Progressive Leasing Breach Litigation	**CONSOLIDATED CLASS ACTION COMPLAINT** Case No. 2:23-cv-00783 Proposed Class Action District Judge David Barlow Magistrate Judge Cecilia M. Romero

Plaintiffs Raymond Dreger, Chad Boyd, Ralph Maddox, Dawn Davis, Richard Guzman Tyler Whitmore, Melanie Williams, Laura Robinson, Allison Ryan, Marty Alexander, and Stephen Hawes ("Plaintiffs") bring this Consolidated Class Action Complaint against Prog Leasing, LLC d/b/a Progressive Leasing ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of Defendant's current and former customers and employees, including, but not limited to, name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

address.

2. According to Defendant's website, it provides "lease-to-own purchase options on items such as furniture, electronics, jewelry, tires & wheels, mobile devices, appliances, mattresses and more."[2]

3. Defendant's Privacy Policy, last updated November 13, 2022, states as follows:

> How Do We Protect Your Information?
>
> We maintain administrative, technical, and physical safeguards intended to protect against the loss, misuse, unauthorized access, and disclosure of Information, including your social security number. Although we take such precautions seriously, it is impossible for us to guarantee the safety and security of your Information. Our policies prohibit the unlawful disclosure of Personal Information. We share Personal Information externally only where federal and state law allows or requires it. Internally, it's our policy to limit the access, use, and disclosure of Personal Information to be in line with the job duties of our associates, as well as applicable law. Please note that we do not ensure or warrant the security of any Information that we collect, and you use the Progressive Platforms and our services and provide us with your Information at your own risk.[3]

4. Defendant's Code of Conduct and Business Ethics states that "[w]e protect company, employee, and customer information" and acknowledges that "Confidential Data includes any information, which is disclosed, may violate the privacy of customers, Company employees…. Special handling and security controls are required."

5. Prior to and through September 11, 2023, Defendant obtained the PII of Plaintiffs and Class Members, including by collecting it directly from Plaintiffs and Class Members.

6. Prior to and through September 11, 2023, Defendant stored the PII of Plaintiffs and

[2] *See* https://progleasing.com/ (last visited Oct. 31, 2023).
[3] Exhibit 1.

Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

7. On or before September 18, 2023, Defendant learned of a data breach on its network that occurred on or around September 11, 2023 (the "Data Breach").

8. Defendant determined that, during the Data Breach, an unknown actor accessed files containing the PII of Plaintiffs and Class Members.

9. On September 21, 2023, Defendant's parent filed a Form 8-K with the Securities and Exchange Commission describing the Data Breach as follows:

> PROG Holdings, Inc. (the "Company") today announced that its Progressive Leasing subsidiary ("Progressive Leasing") recently experienced a cybersecurity incident affecting certain of Progressive Leasing's systems. Promptly after detecting the incident, the Company engaged leading third-party cybersecurity experts and took immediate steps to respond to, remediate and investigate the incident. Law enforcement was also notified. There has been no major operational impact to any of Progressive Leasing's services as a result of the incident and the Company's other subsidiaries have not been impacted.
>
> The Company's investigation into the incident, including identification of the data involved, remains ongoing. Based on preliminary findings from the Company's investigation, the Company believes the involved data contained a substantial amount of personally identifiable information, including social security numbers, of Progressive Leasing's customers and other individuals. Progressive Leasing will provide notice to those individuals whose personally identifiable information was involved in the incident, as well as to regulatory authorities, in accordance with applicable laws.
>
> While no company can ever eliminate the risk of a cyberattack, the Company has taken, and will continue to take, appropriate steps, working with its third-party cybersecurity experts, to further harden its systems to protect against future incidents.

10. On or around September 22, 2023, reports began surfacing on the Internet that the BlackCat/ALPHV ransomware group had acquired PII for 40 million individuals during the Data Breach, including Social Security numbers, bank routing numbers, and checking account numbers.

11. On or around September 23-25, 2023, another report surfaced on the Internet stating that 18 terabytes of data had been exfiltrated during the Data Breach, including "Full Company Data (Internal file shares, Software sources of Leasing Systems), 40 million customer records with full information, including their sensitive banking data," and that "Sample with proof of the exfiltrated data" had been leaked on the dark web.[4]

12. On or around October 23, 2023, Defendant began notifying various states Attorneys General of the Data Breach.

13. On or around October 23, 2023, Defendant began notifying Plaintiffs and Class Members of the Data Breach.

14. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that may have been accessed and/or acquired by an unauthorized actor included name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address.

15. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

16. The PII was compromised due to Defendant's negligent and/or careless acts and

[4] *See* https://hackmanac.com/news/hacks-of-today-23-24-25-09-2023 (last visited Oct. 31, 2023).

omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited more than three months after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

17. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

18. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

19. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures

so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

20. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

21. Raymond Dreger is a citizen of Maine residing in Okmulgee, Oklahoma.

22. Plaintiff Chad Boyd is a citizen of Maine residing in Augusta, Maine.

23. Plaintiff Ralph Maddox is a citizen of Georgia residing in Glenwood, Georgia.

24. Plaintiff Dawn Davis is a citizen of California, residing in Corona, California.

25. Plaintiff Richard Guzman is a citizen of Texas, residing in Brownsville, Texas.

26. Plaintiff Tyler Whitmore is a citizen of Nevada, residing in Henderson, Nevada.

27. Plaintiff Melanie Williams is a citizen of Illinois, residing in Kankakee, Illinois.

28. Plaintiff Laura Robinson is a citizen of Alabama, residing in Silverhill, Alabama.

29. Plaintiff Allison Ryan is a citizen of Washington, residing in Tulalip, Washington.

30. Plaintiff Marty Alexander is a citizen of Virginia, residing in Bristol, Virginia.

31. Plaintiff Stephen Hawes is a citizen of New York, residing in Deerfield, New York.

32. Defendant is a Delaware corporation with a principal place of business in Draper,

Utah.

33. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

34. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

35. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiffs, is a citizen of a state different from Defendant to establish minimal diversity.

36. Under 28 U.S.C. § 1332(d)(10), Defendant is a citizen of Utah because it is a Delaware limited liability company and its principal place of business is in Draper, Utah.

37. The District of Utah has personal jurisdiction over Defendant because it conducts substantial business in Utah and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

38. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

39. Defendant collected the PII of Plaintiffs and Class Members, including Defendant's customers and employees.

40. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

41. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

42. On or about October 23, 2023, Defendant sent Plaintiffs and Class Members a notice of the Data Breach (the "Notice of Data Breach"). Defendant informed Plaintiffs and other Class Members that:

> We are writing to inform you of a data security incident that has affected some of your personal information. We want you to understand what happened, the steps we have taken to address this issue, and additional steps that can be taken to protect your personal information. This letter explains the incident and offers assistance for protecting your information, including complimentary credit and identity monitoring services. We are committed to data protection and deeply regret any concern or inconvenience this incident may have caused.
>
> **What Happened**
>
> On September 11, 2023, we experienced a cybersecurity incident affecting certain Progressive Leasing systems, during which an unauthorized third-party was able to gain access to our network and to certain files containing personal information of some customers and employees. Promptly after detecting the incident, we engaged

> leading cybersecurity experts and launched an investigation. We also notified law enforcement. Our team is working diligently alongside our cybersecurity experts and with law enforcement to investigate and respond to this incident. While our investigation into the incident, including identification of the data involved, remains ongoing, our preliminary findings indicate that the unauthorized third-party first gained access to our network on September 9, 2023.
>
> We are conducting an extensive analysis to determine the individuals whose data was involved in this incident. As part of this review process, on October 9, we identified your personal information among the documents that were acquired without authorization.
>
> **What Information Was Involved**
>
> Based on our investigation and data analysis, the personal information in these stolen documents belonging to you included your name, address, phone number, Social Security number, date of birth, [Extra1], and email address.
>
> **What We Are Doing**
>
> We understand that this is concerning and want to assure you that we have taken prompt action to address this incident. Upon learning of it, we took immediate steps to secure our network environment, hired cybersecurity experts to assist us in our investigation and containment, and notified law enforcement. We are also working with our cybersecurity experts to continue to strengthen our security controls. As an added precaution and to help protect your identity, we have secured the services of Experian to provide credit monitoring, identity restoration, and identity theft protection at no cost to you, as described in this letter.

43. The Notice of Security Incident that Defendant sent to Plaintiffs stated that Plaintiffs' name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address were impacted during the Data Breach.

44. Defendant admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members, including name, address,

phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address.

45. In response to the Data Breach, Defendant claims that "we took immediate steps to secure out network environment, hired cybersecurity experts to assist us in our investigation and containment, and notified law enforcement."[5]

46. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

47. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

48. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

49. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

50. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because

[5] *Id.*

warnings were readily available and accessible via the internet.

51. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[6]

52. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "***[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[7]

53. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[8]

---

[6] FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Jan. 25, 2022).

[7] ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Jan. 25, 2022).

[8] U.S. CISA, Ransomware Guide – September 2020, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_MS ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

54. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

55. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

56. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

57. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members.

58. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members.

59. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

60. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely

maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

61. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[9]

62. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[9] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[10]

63. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

[10] *Id.* at 3-4.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[11]

64. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

[11] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Aug. 23, 2021).

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[12]

65. Given that Defendant was storing the PII of individuals who had worked for Defendant prior to the Data Breach, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

66. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of individuals who worked for Defendant prior to the Data Breach, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

67. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members.

[12] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Aug. 23, 2021).

Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

68. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

69. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

71. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

72. The PII of individuals remains of high value to criminals, as evidenced by the prices

[13] 17 C.F.R. § 248.201 (2013).

[14] *Id*.

they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

74. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[18]

75. Among other forms of fraud, identity thieves may obtain driver's licenses,

---

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[17] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

[18] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

government benefits, medical services, and housing or even give false information to police.

76. The fraudulent activity resulting from the Data Breach may not come to light for years.

77. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

78. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

79. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

80. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

of individuals who would be harmed by the exposure of the unencrypted data.

81. To date, Defendant has offered Plaintiffs and Class Members only one year of credit monitoring, identity restoration, and identity theft protection through Experian. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

82. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

PLAINTIFFS' EXPERIENCES

Plaintiff Raymond Dreger

83. Plaintiff Raymond Dreger is a former customer of Defendant.

84. As a condition of being a customer of Defendant, Plaintiff Dreger was required to provide his PII to Defendant, including his name, address, phone number, social security number, date of birth, income information, and bank account information.

85. At the time of the Data Breach on September 11, 2023, Defendant retained Plaintiff Dreger's PII in its system.

86. Plaintiff Dreger is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PIIin a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Dreger would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

87. Plaintiff Dreger received the Notice Letter, by U.S. mail, directly from Defendant, dated October 23, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name, address, phone number, social

security number, date of birth, income information, and bank account information.

88. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Dreger made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, and contacting companies regarding suspicious activity on his accounts. Plaintiff Dreger has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

89. Plaintiff Dreger further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

90. The Data Breach has caused Plaintiff Dreger to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

91. As a result of the Data Breach, Plaintiff Dreger anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

92. As a result of the Data Breach, Plaintiff Dreger is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

93. Plaintiff Dreger has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Chad Boyd

94. Plaintiff obtained a loan from Defendant in 2022 and received Defendant's Notice of Data Breach on or around October 23, 2023. The notice stated that Plaintiff's personal information, including name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit, and email address, were impacted by the Data Breach.

95. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

96. In late September 2023, after the Data Breach, Plaintiff noticed unauthorized charges on his debit card. He filed a dispute with the bank but has not been reimbursed. These charges caused his account to be overdrawn and he missed bill payments as a result.

97. In October 2023, Plaintiff noticed approximately fifteen (15) hard inquiries on his credit report, all of which were inaccurate.

98. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

99. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

100. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and

passwords for his various online accounts.

101. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

102. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

103. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Ralph Maddox

104. Plaintiff Ralph Maddox is a current Progressive customer and has been for approximately three years.

105. In order to obtain financial services at Progressive, he was required to provide his PII to Defendant, including his name, date of birth, Social Security number, contact information, and other sensitive information.

106. At the time of the Data Breach—from approximately September 9, 2023 through September 11, 2023— Defendant retained Plaintiff's PII in its system.

107. Plaintiff Maddox is very careful about sharing his sensitive PII. Mr. Maddox stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

108. Plaintiff Maddox received the Notice Letter, by U.S. mail, directly from Defendant, dated October 23, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his full name, address, phone number, Social

Security number, date of birth, monthly gross income, and email address.

109. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Maddox made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: such contacting credit bureaus to place freezes on his credit, changing passwords and resecuring his own computer network, and placing security measures on his financial accounts. Plaintiff Maddox has spent significant time on activities in response to the Data Breach—valuable time Plaintiff Maddox otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

110. Plaintiff Maddox suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

111. Plaintiff Maddox further suffered actual injury in the form of his PII being disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

112. Plaintiff Maddox also suffered actual injury in the form experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

113. The Data Breach has caused Plaintiff Maddox to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

114. As a result of the Data Breach, Plaintiff Maddox anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Maddox is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

115. Plaintiff Maddox has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Dawn Davis

116. Plaintiff Davis has been a customer of Progressive for approximately four years and currently holds an active lease.

117. To obtain financial services at Progressive, she was required to provide her PII to Defendant, including her name, date of birth, Social Security number, contact information, and other sensitive information.

118. At the time of the Data Breach—from approximately September 9, 2023 through September 11, 2023— Defendant retained Plaintiff Davis's PII in its system.

119. Plaintiff Davis received the Notice Letter, by U.S. mail, directly from Defendant, dated October 23, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her full name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, and email address.

120. This unauthorized access of Plaintiff Dawn's personal information, which resulted

from Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, has harmed Plaintiff Davis.

121. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Davis made reasonable efforts to mitigate the impact of the Data Breach, which required her to expend significant time—valuable time Plaintiff Davis otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

122. Plaintiff Davis suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

123. Plaintiff Davis also suffered actual injury in the form experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

124. The Data Breach has caused Plaintiff Davis to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

125. As a result of the Data Breach, Plaintiff Davis anticipates spending considerable

time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Davis is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

126. Plaintiff Davis has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

127. Plaintiff Davis would not have provided her PII to Defendant and/or would have switched to another lease and rental provider if she had been aware of Defendant's inadequate computer and data security practices to safeguard its customers' personal and financial information from theft.

128. On November 13, 2023, Plaintiff Davis provided written notice to Defendant, identifying the specific provisions of the California Consumer Privacy Act that she alleges have been or are being violated. More than 30 days have passed since this written notice, and Defendant has failed to cure this breach pursuant to California Civil Code §1798.150(b). Accordingly, as set forth below, Plaintiff and the California subclass of similarly-situated individuals seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per class member.

Plaintiff Richard Guzman

129. Plaintiff Guzman has been a customer of Progressive Leasing since January 2022. In January 2022, he leased jewelry through Progressive Leasing, which was paid off in late 2022. In or about September 2023, Mr. Guzman leased a laptop through Progressive Leasing, which he has paid off.

130. Plaintiff Guzman suffered, and continues to suffer from, actual and imminent

identity theft and misuse of his PII as a direct and/or proximate result of Progressive Leasing actions and inactions.

131. Progressive Leasing's conduct, which allowed the Data Breach to occur, caused Plaintiff Guzman significant injuries and harm, including but not limited to, the following—Plaintiff Guzman immediately devoted (and must continue to devote) time, energy, and money to: closely monitor his bills, records, and credit and financial accounts and more carefully screen and scrutinize phone calls, emails, and other communications to ensure that he is not being targeted in a social engineering or spear phishing attack. Plaintiff Guzman has taken or will be forced to take these measures in order to mitigate his potential damages that are fairly traceable to the Data Breach.

132. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, in addition to the increased, imminent, and substantial risk of a future data breach and harm, Plaintiff Guzman will need to maintain these heightened measures for years, and possibly his entire life.

133. Plaintiff Guzman greatly values his privacy, especially while receiving financial services. He would not have obtained financial services from Progressive Leasing, or paid the amount he did to receive such, had he known that Progressive Leasing would negligently fail to adequately protect his PII. Indeed, Plaintiff Guzman paid Progressive Leasing for financial services with the expectation that Progressive Leasing would keep his PII secure and inaccessible from unauthorized parties, as promised by Progressive Leasing.

134. Plaintiff Guzman is also at a continued imminent and substantial risk of harm because his PII remains in Progressive Leasing systems, which have already been shown to be susceptible to compromise and attack and are subject to an increased and imminent future attack.

135. As a result of the Data Breach, and in addition to the time Plaintiff Guzman has spent and anticipates spending to mitigate the impact of the Data Breach on his life, Plaintiff Guzman also suffered emotional distress from the public release of his PII, which he believed would be protected from unauthorized access and disclosure. The emotional distress he experienced, and will continue to experience, includes anxiety and stress resulting from the unauthorized bad actors viewing, selling, and misusing his PII for the purposes of identity theft and fraud.

136. Additionally, Plaintiff Guzman has suffered damage to and diminution in the value of his highly sensitive and confidential PII—a form of property that Plaintiff Guzman provided and entrusted to Progressive Leasing, and which was compromised as a result of the Data Breach Progressive Leasing failed to prevent. Plaintiff Guzman has also suffered a violation of his privacy rights as a result of Progressive Leasing's unauthorized disclosure of his PII.

137. The free credit monitoring and identity restoration services offered by Progressive Leasing after the Data Breach were and continue to be ineffective because these services would have shared Plaintiff Guzman's information with third parties and could not guarantee complete privacy of his sensitive information.

138. The time spent dealing with these incidents resulting from the Data Breach is time Mr. Guzman otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Progressive Leasing's direction. Indeed, in the notice letter Plaintiff received, Progressive Leasing directed Plaintiff to spend time by reviewing his accounts and credit reports for unauthorized activity.

Plaintiff Tyler Whitmore

139. Plaintiff Tyler Whitmore is a resident and citizen of the State of Nevada. Plaintiff

Whitmore is a customer of Progressive Leasing. While he was temporarily in Tempe, Arizona in May of 2023, he applied for a loan at a store through Progressive Leasing. Ultimately he was approved for the loan but did not borrow with Progressive Leasing. However, he did share with it his PII.

140. Plaintiff Whitmore received a Notice of Data Breach Letter from Progressive Leasing dated October 23, 2023. It states that the breached files included his "name, address, phone number, Social Security number, date of birth, bank account number, monthly gross income, credit limit and email address."

141. Plaintiff Whitmore has never been part of a data breach and is not aware of any time other than this that his Social Security Number, bank and income information was exposed, as he diligently protects and maintains his PII.

142. Plaintiff Whitmore is especially alarmed and anxious that his Social Security number and income information was identified as among the breached data on Progressive Leasing's computer system.

143. Plaintiff Whitmore is reasonably concerned that his PII has now been exposed to bad actors. As a result, he has taken multiple steps to avoid identity theft, including considering signing up for the credit monitoring services, more often checking his Credit Karma and possibly going back to paying for that service, considering freezing his credit, changing his bank account and passwords, setting up notices and reports and carefully reviewing all his accounts.

144. In addition, Plaintiff Whitmore now receives an increased number of spam texts, including text and call from international numbers as well, that he reasonably and temporally attributes to the Data Breach.

145. Plaintiff Whitmore has spent as many as forty (40) hours to date obtaining and

reviewing the results of his credit monitoring service and additional monitoring of personal and financial accounts as a result of the Data Breach. The time spent dealing with these incidents resulting from the Data Breach is time he otherwise would have spent on other activities, such as work and/or recreation. Moreover, the time Plaintiff lost was spent at Defendant's recommendations.

146. Plaintiff Whitmore is aware that cybercriminals often sell PII, and one stolen, it is likely to be abused months or even years after Progressive Leasing's Data Breach.

147. Had Plaintiff Whitmore been aware that Progressive Leasing's computer systems were not secure, he would not have trusted Progressive Leasing with his PII.

Plaintiff Melanie Williams

148. When Plaintiff Williams first became a customer of Progressive Leasing, she was required to provide it with substantial amounts of her PII.

149. On or about October 23, 2023, Plaintiff Williams received a letter entitled "Notice of Data Breach" which told her that her PII had been acquired during the Data Breach. The notice letter informed her that the PII compromised included her "name, address, phone number, social security number, date of birth, bank account number, monthly gross income, credit limit, and email address."

150. The notice letter offered Plaintiff Williams only one year of credit monitoring services – an amount that is insufficient given that Plaintiff Williams will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her PII.

151. Plaintiff Williams would not have provided her PII to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard

its customers' personal information from theft, and that those systems were subject to a data breach.

152. Plaintiff Williams suffered actual injury in the form of having her PII compromised and/or stolen as a result of the Data Breach. In fact, Plaintiff Williams was recently alerted to her information, including the PII compromised in the Data Breach, being found on the dark web.

153. Plaintiff Williams also suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Williams entrusted to Defendant for the purpose of receiving leasing services from Defendant and which was compromised in, and as a result of, the Data Breach.

154. Plaintiff Williams suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her PIIbeing placed in the hands of criminals.

155. Plaintiff Williams has a continuing interest in ensuring that her PII, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

156. As a result of the Data Breach, Plaintiff Williams made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Williams has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

157. As a result of the Data Breach, Plaintiff Williams has suffered anxiety as a result of the release of her PII to cybercriminals, which PII she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties

viewing, selling, and/or using her PII for purposes of committing cyber and other crimes against her. Plaintiff Williams is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

158. Plaintiff Williams also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Williams; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

159. Plaintiff Williams anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Laura Robinson

160. When Plaintiff Robinson first became a customer of Progressive Leasing, she was required to provide it with substantial amounts of her PII.

161. On or about October 23, 2023, Plaintiff Robinson received a letter entitled "Notice of Data Breach" which told her that her PII had been acquired during the Data Breach. The notice letter informed her that the PII compromised included her "name, address, phone number, social security number, date of birth, bank account number, monthly gross income, credit limit, and email address."

162. The notice letter offered Plaintiff Robinson only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Robinson will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her PII.

163. Plaintiff Robinson suffered actual injury in the form of the fraudulent misuse of her compromised PII leading to her bank accounts being frozen without her authorization, with all money in those accounts drained without explanation. Plaintiff Robinson no longer has access to these accounts, nor the funds that were in them.

164. Plaintiff Robinson also suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of additional fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

165. Plaintiff Robinson would not have provided her PII to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

166. Plaintiff Robinson suffered actual injury in the form of having her PII compromised and stolen as a result of the Data Breach.

167. Plaintiff Robinson suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Robinson entrusted to Defendant for the purpose of receiving leasing services from Defendant and which was compromised in, and as a result of, the Data Breach.

168. Plaintiff Robinson suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her PII being placed in the hands of criminals.

169. Plaintiff Robinson has a continuing interest in ensuring that her PII, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

170. As a result of the Data Breach, Plaintiff Robinson made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Robinson has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

171. As a result of the Data Breach, Plaintiff Robinson has suffered anxiety as a result of the release of her PIIn to cybercriminals, which PIIshe believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of committing cyber and other crimes against her. Plaintiff Robinson is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

172. Plaintiff Robinson also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Robinson; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

173. As a result of the Data Breach, Plaintiff Robinson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Allison Ryan

174. When Plaintiff Ryan first became a customer of Progressive Leasing, she was required to provide it with substantial amounts of her PII.

175. On or about October 23, 2023, Plaintiff Ryan received a letter entitled "Notice of Data Breach" which told her that her PII had been acquired during the Data Breach. The notice letter informed her that the PII compromised included her "name, address, phone number, social security number, date of birth, bank account number, monthly gross income, credit limit, and email address."

176. The notice letter offered Plaintiff Ryan only one year of credit monitoring services – an amount that is insufficient given that Plaintiff Ryan will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her PII.

177. Plaintiff Ryan would not have provided her PII to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

178. Plaintiff Ryan suffered actual injury in the form of having her PII compromised and/or stolen and fraudulently misused as a result of the Data Breach. Specifically, since receiving the Notice, Plaintiff Ryan has already experienced at least two hard inquiries on her credit, received receipts sent to her email relating to items she never purchased, and was forced to spend time getting a new credit card after noticing a series of unauthorized charges on her prior credit card.

179. Plaintiff Ryan suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Ryan entrusted to Defendant for the purpose of receiving leasing services from Defendant and which was compromised in, and as a result of, the Data Breach.

180. Plaintiff Ryan suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her PII being placed in the hands of criminals.

181. Plaintiff Ryan has a continuing interest in ensuring that her PII, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

182. As a result of the Data Breach, Plaintiff Ryan made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Ryan has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

183. As a result of the Data Breach, Plaintiff Ryan has suffered anxiety as a result of the release of her PII to cybercriminals, which PII she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII for purposes of committing cyber and other crimes against her. Plaintiff Ryan is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

184. Plaintiff Ryan also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Ryan; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

185. Plaintiff Ryan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Marty Alexander

186. Plaintiff Marty Alexander is a former customer of Defendant.

187. As a condition of being a customer of Defendant, Plaintiff Alexander was required

to provide his PII to Defendant, including his name, address, phone number, social security number, date of birth, bank account number, monthly gross income, and email address.

188. At the time of the Data Breach on September 11, 2023, Defendant retained Plaintiff Alexander's PII in its system.

189. Plaintiff Alexander is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Alexander would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

190. Plaintiff Alexander received the Notice Letter, by U.S. mail, directly from Defendant, dated October 23, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including his name, address, phone number, social security number, date of birth, bank account number, monthly gross income, and email address.

191. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Alexander made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, researching credit monitoring and/or identity theft protection services, enrolling in credit monitoring and/or identity theft protection services, reviewing credit reports, reviewing account statements, and mitigating fraud/identity theft. Plaintiff Alexander has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

192. Plaintiff Alexander further suffered actual injury in the form of: (i) attempted identity theft, (ii) lost time related to monitoring his accounts for fraudulent activity; (iii) loss of privacy due to his PII being exposed to cybercriminals; (iv) loss of the benefit of the bargain because Defendant did not adequately protect his PII; (v) severe emotional distress because identity thieves now possess his PII; (vi) exposure to increased and imminent risk of fraud and identity theft now that his PII has been exposed; (vii) the loss in value of his PII due to his PII being in the hands of cybercriminals who can use it at their leisure; (viii) actual misuse of his PII; and (ix) other economic and non-economic harm.

193. Specifically, Plaintiff Alexander has received multiple notifications indicating that an unauthorized user has attempted to obtain loans with Wells Fargo, American Express, the Bank of Missouri, and Community Bank using his PII.

194. First, on September 14, 2023, Plaintiff Alexander, through CreditKarma, received an alert that a Wells Fargo account was attempted to be opened in his name. Specifically, a hard inquiry into Plaintiff's credit was placed by Wells Fargo, which is done by a lender in response to a borrower's application to apply for a mortgage, loan, credit card, or line of credit. Plaintiff never applied for a loan of any kind with Wells Fargo.

195. Next, on September 17, 2023, Plaintiff Alexander, through CreditKarma, received an alert that an account with The Bank of Missouri was attempted to be opened in his name. Specifically, a hard inquiry into Plaintiff's credit was placed by The Bank of Missouri, which is done by a lender in response to a borrower's application to apply for a mortgage, loan, credit card, or line of credit. Plaintiff never applied for a loan of any kind with The Bank of Missouri.

196. Next, on October 1, 2023, Plaintiff Alexander, through Experian, received an alert that an American Express account was attempted to be opened in his name. Specifically, a hard

inquiry into Plaintiff's credit was placed by American Express, which is done by a lender in response to a borrower's application to apply for a mortgage, loan, credit card, or line of credit. Plaintiff never applied for a loan of any kind with American Express.

197. Finally, on February 21, 2024, Plaintiff Alexander, through Experian, received an alert that a Community Bank account was attempted to be opened in his name. Specifically, a hard inquiry into Plaintiff's credit was placed by Community Bank, which is done by a lender in response to a borrower's application to apply for a mortgage, loan, credit card, or line of credit. Plaintiff never applied for a loan of any kind with Community Bank.

198. The Data Breach and multiple hard inquiries has negatively affected Plaintiff's credit and has caused Plaintiff Alexander to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

199. As a result of the Data Breach, Plaintiff Alexander anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

200. As a result of the Data Breach, Plaintiff Alexander is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

201. Plaintiff Alexander has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Stephen Hawes

202. Plaintiff Hawes is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the

internet or any other unsecured source. Plaintiff Hawes stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Hawes diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

203. Plaintiff Hawes only allowed Defendant to maintain, store, and use his PII because he believed that Defendant would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendant at the time of the Data Breach.

204. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff Hawes suffered injury from a loss of privacy.

205. Plaintiff Hawes has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff Hawes entrusted to Defendant. This information has inherent value that Plaintiff Hawes was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

206. Upon information and belief, Plaintiff's PII has already been stolen and misused as he has experienced a marked increase in the amount of spam notifications, texts, calls, and emails Plaintiff Hawes has received, including specific phishing attempts targeting even more compromising information.

207. The Data Breach has also caused Plaintiff Hawes to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and/or misuse resulting from his PII being placed in the hands of criminals.

208. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff Hawes to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Data Breach Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

209. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff Hawes to suffer stress, fear, and anxiety.

210. Plaintiff Hawes has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

V. CLASS ALLEGATIONS

211. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

212. The Nationwide Class that Plaintiffs seeks to represent is defined as follows:

> All individuals whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around October 23, 2023 (the "Nationwide Class").

213. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs asserts claims on behalf of a separate subclass, defined as follows:

> All individuals who were customers of Defendant or before September 11, 2023, and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or

> around October 23, 2023 (the "Customer Subclass") (collectively, with the Nationwide Class, "the Classes").

214. Pursuant to Rule 23, Plaintiff Dawn Davis asserts claims on behalf of a California subclass, defined as follows:

> All California residents whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around October 23, 2023 (the "California Subclass").

215. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

216. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

217. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant reported to the Maine Attorney General that 193,055 individuals were impacted in the Data Breach.

218. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and

Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

219. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

220. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

221. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

222. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their

common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

223. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs was exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

224. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

225. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

226. Unless a Class-wide injunction is issued, Defendant may continue in its failure to

properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

227. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

228. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

229. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 to 228 above.

230. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

231. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

232. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

233. Defendant also had a duty to exercise appropriate clearinghouse practices to remove

from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

234. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

235. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiffs' and the Nationwide Class's confidential PII in the course of its business practices.

236. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

237. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

238. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

239. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to

Defendant.

240. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

241. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

242. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

243. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

244. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

245. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

246. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

247. Defendant failed to heed industry warnings and alerts to provide adequate

safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

248. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

249. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

250. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

251. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

252. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

253. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual

identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

254. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

255. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

256. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Customer Subclass)

257. Plaintiffs and the Customer Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 to 228 above.

258. Defendant's Privacy Policy states that it "maintain[s] administrative, technical, and physical safeguards intended to protect against the loss, misuse, unauthorized access, and disclosure of Information, including your social security number" and that it "take[s] such precautions seriously."

259. In obtaining loans or other products or services from Defendant, Plaintiffs and the Customer Subclass provided and entrusted their PII to Defendant.

260. Defendant required Plaintiffs and the Customer Subclass to provide and entrust their PII as condition of obtaining loans or other products or services from Defendant.

261. As a condition of obtaining loans or other products or services from Defendant, Plaintiffs and the Customer Subclass provided and entrusted their PII. In so doing, Plaintiffs and the Customer Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the Customer Subclass if their PII had been compromised or stolen.

262. Plaintiffs and the Customer Subclass fully performed their obligations under the implied contracts with Defendant.

263. Defendant breached the implied contracts it made with Plaintiffs and the Customer Subclass by failing to maintain administrative, technical, and physical safeguards intended to

protect against the loss, misuse, unauthorized access, and disclosure of their PII, failing to take such precautions seriously, and otherwise failing to safeguard and protect their PII.

264. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Customer Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

265. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Customer Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

266. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 to 228 above.

267. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

268. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

269. Plaintiffs and the Nationwide Class's have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Nationwide Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiffs.

270. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Nationwide Class;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

271. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government

regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

f. regularly test its systems for security vulnerabilities, consistent with industry standards;

g. implement an education and training program for appropriate employees regarding cybersecurity.

272. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

273. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

274. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at

Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT IV
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
CAL. CIVIL CODE SEC. 1798.150, ET SEQ.
(On Behalf of Plaintiff Davis and the California Class)

275. Plaintiff Davis incorporates the allegations contained in the foregoing paragraphs as though repeated here.

276. Plaintiff Davis brings this cause of action on behalf of herself and the California Subclass.

277. California Civil Code section 1798.150, subdivision (a)(1), provides,

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
>
> (B) Injunctive or declaratory relief.
>
> (C) Any other relief the court deems proper.

278. Defendant took possession, retained, stored, and maintained the nonencrypted and nonredacted PII of Plaintiff Davis and the California Subclass. Defendant collects or receives such information and determines the purposes and means of the processing of such PII.

279. As a result of the Data Breach, nonredacted and nonencrypted PII of Plaintiff Davis and the California Subclass members was compromised, accessed, and subject to exfiltration, theft or disclosure.

280. The Data Breach subjected Plaintiff Davis and the California Subclass members to an unauthorized access and exfiltration, theft, or disclosure of their nonencrypted and nonredacted PII, including, but not limited to, PII that falls within the definition of subparagraph (A) of paragraph (1) of subdivision (d) of Civil Code section 1798.81.5.

281. The Data Breach was a result of Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

282. Due to the Data Breach, Plaintiff Davis and the California Subclass members are entitled to recover actual damages. Pursuant to California Civil Code § 1798.150, Plaintiff Davis, on behalf of herself and all other members of the California subclass, seeks actual damages.

283. On November 13, 2023, Plaintiff Davis provided written notice to Defendant, identifying the specific provisions of the CCPA that she alleges have been or are being violated. More than 30 days have passed since this written notice, and Defendant has failed to cure this breach pursuant to California Civil Code §1798.150(b). Accordingly, Plaintiff and the California subclass of similarly-situated individuals seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per class member.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Customer Subclass, and the California Subclass, and appointing Plaintiffs and his Counsel to represent such Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct

testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of statutory damages for Plaintiff Davis and the California Subclass pursuant to California Civil Code section 1798.150;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: April 19, 2024

Respectfully Submitted,

/s/ *Ryan D. Maxey*

Daniel Srourian, Esq. [*Admitted Pro Hac Vice*]
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
Telephone: (213) 474-3800
Facsimile: (213) 471-4160
Email: daniel@slfla.com

Patrick A. Barthle II*
Florida Bar No. 99286
pbarthle@ForThePeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 229-4023
Facsimile: (813) 222-4708

Ryan D. Maxey*
Florida Bar No.: 0059283
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
Telephone: (813) 448-1125
Email: ryan@maxeyfirm.com

Attorneys for Plaintiffs and the Proposed Class

Jared D. Scott (#15066)
ANDERSON & KARRENBERG
50 West Broadway, #600
Salt Lake City, UT 84101-2035

Telephone: (801) 534-1700
jscott@aklawfirm.com

Richard Lyon
rick@dovel.com
DOVEL & LUNER, LLP
201 Santa Monica Blvd., Suite 600
Santa Monica, California 90401
Telephone: (310) 656-7066

Attorneys for Plaintiff Dawn Davis

Jared D. Scott (#15066)
ANDERSON & KARRENBERG
50 West Broadway, #600
Salt Lake City, UT 84101-2035
Telephone: (801) 534-1700
jscott@aklawfirm.com

Kenneth J. Grunfeld (Pro Hac Vice)
KOPELOWITZ OSTROW, P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Telephone: (954) 525-4100
grunfeld@kolawyers.com

Attorneys for Plaintiff Tyler Whitmore

Jason R. Hull [11202]
jhull@mohtrial.com
MARSHALL OLSON & HULL, PC
Newhouse Building
Ten Exchange Place, Suite 350
Salt Lake City, Utah 84111
Telephone: 801.456.7655

Mason A. Barney*
mbarney@sirillp.com
Tyler J. Bean*
tbean@sirillp.com
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Telephone: 212.532.1091

Attorneys for Plaintiffs Williams, Robinson, and Ryan

Charles H. Thronson
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, Utah 84111
Telephone: (801) 532-1234

William B. Federman
wbf@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560

Attorneys for Plaintiff Alexander

Ashton J. Hyde
YOUNKER HYDE MACFARLANE, PPLC
250 E. 200 South, Suite 1100
Salt Lake City, UT 84111
Telephone: (801) 335-6467
ashton@yhmlaw.com

Terence R. Coates
Dylan J. Gould
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 665-0204
tcoates@msdlegal.com
dgould@msdlegal.com

Counsel for Plaintiff Stephen Hawes

**pro hac vice applications pending*

CERTIFICATE OF SERVICE

I hereby certify that on April 19, 2024, I electronically filed the foregoing document using the electronic filing system, which will send notification of such filing to all attorneys of record.

/s/ Ryan D. Maxey
Ryan D. Maxey